



VU Research Portal

Het recht geketend: Smart contracts: de oplossing voor gezeur, gedoe en onzekerheid
van der Linden, M.

published in

Tijdschrift voor Internetrecht
2018

document version

Publisher's PDF, also known as Version of record

document license

Article 25fa Dutch Copyright Act

[Link to publication in VU Research Portal](#)

citation for published version (APA)

van der Linden, M. (2018). Het recht geketend: Smart contracts: de oplossing voor gezeur, gedoe en onzekerheid. *Tijdschrift voor Internetrecht*, 11(2), 59-63. [14970]. <https://denhollander.info/artikel/14970>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:

vuresearchportal.ub@vu.nl

Het recht geketend: Smart contracts: dé oplossing voor gezeur, gedoe en onzekerheid?

mr. M. van der Linden¹

1. Inleiding

Smart contracts: dé oplossing voor alle problemen? Wie wil dat nou niet. Of is het alleen maar ‘gekkigheid’, waar een paar enthousiastelingen veel aandacht mee genereren en geld mee verdienen? Of iets daar tussenin: het heeft bepaalde voordelen en soms is het handig? Als oudere jongere neig ik naar dat laatste; bekijk ik dit soort nieuwe ontwikkelingen met de nodige scepsis. Lijkt het niet verdacht veel op oude wijn in nieuwe zakken? Ik wil het eigenlijk tot op het bot begrijpen voordat ik me aan een oordeel waag.

In dit artikel wil ik de lezer meenemen in mijn zoektocht naar wat ik nou moet vinden van zogenaamde smart contracts, geïmplementeerd op de blockchain. Ik probeer door alle ronkend enthousiaste praatjes, ongefundeerde claims en in mooie woorden vermomde onwetendheid te achterhalen wát het nou écht is en hoe het nou écht werkt. Vervolgens wil ik proberen te bedenken waarom contractspartijen hun overeenkomst op deze manier vorm zouden willen geven. En wat mogelijke andere bruikbare manieren kunnen zijn om deze technologie te gebruiken. Onvermijdelijk stuiten we op vragen die we samenvegen onder de noemer ‘uitdagingen voor het recht’. Die zal ik in dit artikel alleen aanduiden, in een volgend artikel probeer ik ze in kaart te brengen.

2. Hoe werkt het

Een smart contract is een blockchain-toepassing. Dus om te kunnen begrijpen hoe het werkt moeten we de techniek van de blockchain induiken. Zoals ieder stuk over privacy begint met Warren en Brandeis, zo begint een blockchain-verhandeling altijd met het verhaal van Satoshi Nakamoto. En daar hebben we meteen een kenmerk te pakken: anonimiteit. Satoshi Nakamoto is een pseudoniem, en niemand (behalve de persoon of personen in kwestie zelf natuurlijk) weet zeker wie erachter zit.

Satoshi Nakamoto schreef in 2008 een paper dat beschouwd kan worden als het eindpunt van de jarenlange zoektocht naar een manier om anoniem en betrouwbaar via internet te kunnen betalen,² en het beginpunt van de ontwikkeling van blockchain.³ Betalen via internet werd eigenlijk pas verrassend laat mogelijk met diensten als PayPal en (in Nederland) iDeal. Daarvoor was er alleen de betaling met een creditcard – ontoegankelijk (want niet iedereen heeft zomaar een creditcard), duur en riskant voor beide partijen. Een tussenpersoon (bank of andere financiële dienstverlener) was dus altijd nodig: een zogenaamde trusted third party (TTP). Die trust in die third party was niet altijd van harte, maar je moest wel, er was immers geen keuze. En in 2008 bleek dat dat vertrouwen niet altijd terecht was – en de ruggespraak van onze economie moest in het algemeen belang, en dus met publieke middelen, overeind gehouden worden. En bovendien is een TTP kwetsbaar voor hacken en dDos aanvallen en zo.

In de fysieke wereld kunnen we contant betalen: snel, efficiënt,⁴ anoniem. Zoals we uit de privacy literatuur weten is anonimiteit niet alleen nuttig als je iets te verbergen hebt, maar ook als jouw identiteit niet relevant is. En door de fysieke verschijningsvorm van contant geld (munten of bankbiljet-

-
2. Zie onder andere: R.C. Merkle, ‘Protocols for public key cryptosystems’, in: *Security and Privacy*, 1980 IEEE Symposium on (p. 122-122). IEEE. (https://www.researchgate.net/profile/Ralph_Merkle/publication/220713913_Protocols_for_Public_Key_Cryptosystems/links/00b495384ecda07784000000/Protocols-for-Public-Key-Cryptosystems.pdf); D. Chaum, (1983) ‘Blind Signatures for Untraceable Payments’, in: D. Chaum, R.L. Rivest & A.T. Sherrman (eds), *Advances in Cryptology*, Boston: Springer, MA (https://doi.org/10.1007/978-1-4757-0602-4_18); W. Dai, ‘b-money’, <http://www.weidai.com/bmoney.txt>, 1998; F.D. Garcia & J.H. Hoepman (2005), ‘Off-Line Karma: A Decentralized Currency for Peer-to-peer and Grid Applications’, in: J. Ioannidis, A. Keromytis & M. Yung (eds), *Applied Cryptography and Network Security*, ACNS 2005. Lecture Notes in Computer Science, vol 3531. Berlin: Springer, Heidelberg (https://doi.org/10.1007/11496137_25).
 3. S. Nakamoto, (2008), *Bitcoin: A peer-to-peer electronic cash system*, <https://bitcoin.org/bitcoin.pdf>.
 4. Lage transactiekosten behalve als je grote hoeveelheden muntjes op je bankrekening wilt zetten.

1. Tina van der Linden is universitair docent Law Ethics and Technology aan de Vrije Universiteit Amsterdam en redacteur van dit blad.

ten) kun je hetzelfde geld niet twee keer uitgeven. Dit 'double spending problem' was de grote uitdaging voor internetgeld: natuurlijk kun je reeksen van codes maken en afspreken om daar een bepaalde waarde aan toe te kennen, maar hoe weet je zeker dat de codes die jij ontvangt niet al eerder door dezelfde persoon uitgegeven zijn om bij iemand anders ook iets te kopen? Tom Poes verzint een list. Satoshi Nakamoto verzint de blockchain door drie al langer bestaande technieken te combineren: peer-to-peer technologie, asymmetrische encryptie en hashing.

Peer-to-peer technologie is vooral bekend uit de file-sharing wereld: er is geen centraal knooppunt maar een netwerk van deelnemers, zogenaamde peers, die allemaal potentieel met elkaar verbonden zijn. In theorie zijn alle peers gelijkwaardig.

Asymmetrische encryptie maakt gebruik van een briljante wiskundige truc: een manier om gegevens te versleutelen met de ene sleutel, waarbij die gegevens uitsluitend met de andere sleutel te ontsleutelen zijn, en tegelijkertijd die twee sleutels (die uiteraard wel aan elkaar gerelateerd zijn) niet uit elkaar te herleiden zijn.

Hashing is een manier om gegevens te verzegelen. Door een bewerking op een verzameling van gegevens los te laten wordt een zogenaamde hash gecreëerd, een code. Elke wijziging in de gegevens, ook al is die nog zo miniem, resulteert in een totaal andere hash-code. Kortom een correcte hash garandeert dat de gegevens ongewijzigd zijn.

Het werkt dan conceptueel als volgt. De transacties in het netwerk van deelnemende peers worden bloksgewijs vastgelegd in een traditioneel grootboek, in digitale vorm natuurlijk. Alle peers hebben de complete versie van dit grootboek op hun computer staan. Dat is de uitgangspositie.

Dan vinden er transacties plaats tussen de peers. De ene peer betaalt aan de andere door een bericht het netwerk in te sturen (dus naar alle peers), versleuteld met asymmetrische encryptie, met als inhoud dat zij een bepaald bedrag aan die ander betaalt. Dat kan natuurlijk alleen als zij ook minimaal over dat bedrag beschikt. En dat kan aan de hand van het grootboek door alle peers in het netwerk geverifieerd worden.

Een aantal geverifieerde (en dus goedgekeurde) transacties wordt samengevoegd tot een nieuw blok, dat aan het grootboek wordt toegevoegd. Dát is wat 'minen' genoemd wordt: een nieuw blokje 'vinden' en vastklikken als de nieuwe schakel aan het al bestaande grootboek. Dat houdt in dat je een nieuwe hash moet vinden. De gegevens voor die nieuwe hash omvatten: de hash van het vorige blok (zo weet je zeker dat het 'past'), de verzameling van goedgekeurde transacties van dit blok, én een getal genaamd 'nonce', number used once. De resulterende hash moet onder een bepaald maximum uitkomen, die steeds lager wordt, zodat het steeds moeilijker wordt om er nog onderdoor te komen. Minen komt dus neer op het eindeloos uitproberen van getallen als nonce, totdat je er eentje hebt die, samen met de andere gegevens uit het blok, resulteert in een hash die laag genoeg is. Het is net als met het op-

lossen van een Sudoku: het vinden van de oplossing is lastig en vergt veel doorzettingsvermogen en een beetje geluk, maar het vaststellen dat de gevonden oplossing de juiste is, is een eitje. Minen kost dus veel, en steeds meer, rekenkracht, en daarmee elektriciteit: 'proof-of-work'. Maar het levert ook wat op: een beloning in de digitale valuta van de desbetreffende blockchain.

Het nieuwe blok wordt toegevoegd aan de ketting, het grootboek wordt bijgewerkt, alle peers ontvangen de nieuwe versie en het verhaal kan van voren af aan beginnen. Blockchain is dus: een manier om data op te slaan, gedistribueerd in een peer-to-peer netwerk met asymmetrische encryptie en hashing als beveiliging. En het kan gebruikt worden voor toepassingen waarbij het gaat om overdracht van zaken die een bepaalde waarde vertegenwoordigen: niet alleen cryptocurrencies (digitale valuta), maar ook andere handelsoBJECTEN – en dan hebben we het over smart contracts.

En zo zijn de grote uitdagingen van betalen via internet opgelost. Het kan anoniem, althans pseudoniem, via een account in het netwerk – dat natuurlijk aan het IP-adres van een computer gekoppeld is maar dat is vrij eenvoudig te maskeren. Het double spending-probleem is opgelost omdat alleen geverifieerde transacties doorgang vinden. Trusted third parties zijn niet meer nodig: in het netwerk van peers wordt het vertrouwen gecreëerd door de onomstotelijkheid van waterdichte encryptie en hashes. Iedereen blij. Of toch niet?

Nakamoto introduceerde met zijn paper de eerste toepassing van blockchain-technologie: de Bitcoin. Een op de internet-infrastructuur gebaseerde manier om peer-to-peer, anoniem en wereldwijd waarde over te dragen. Waar wordt dat, natuurlijk, in eerste instantie en vooral voor gebruikt? Natuurlijk voor transacties die het daglicht niet kunnen verdragen (drugs, wapens, kinderporno), voor afpersing (Wannacry), voor witwassen van crimineel geld. Er zijn geen banken bij betrokken, het is anoniem en wereldwijd, dus er is niet echt een aanknopingspunt voor handhaving van een nationaal rechtssysteem of financieel toezicht. Grillig koersverloop trekt speculanten aan waardoor Bitcoin tot een soort piramidespel wordt. Bitcoin exchanges (wisselkantoren) en handelsplatformen op het Dark Web worden opgerold, verdwijnen in het niets – criminelen zijn niet te vertrouwen.⁵ En natuurlijk, de Bitcoin blockchain is pas de eerste toepassing van deze techniek, dus de techniek is ook nog lang niet uitontwikkeld en kan op veel punten gewijzigd en verbeterd worden.

Verdere ontwikkeling

Op het basisidee van gedistribueerde gegevensopslag van versleutelde transacties die via hashes rotsvast aan elkaar gelinkt zijn, zijn natuurlijk variaties en daarmee andere toepassingen mogelijk.

5. D. Gerard, 'Attack of the 50 Foot Blockchain: Bitcoin, Blockchain', *Ethereum & Smart Contracts*, CreateSpace: Independent Publishing Platform 2017.

Om te beginnen hoeft je natuurlijk niet zomaar iedereen toe te laten tot jouw blockchain. Je kunt best een eigen clubje oprichten, met een eigen blockchain en een toelatingsprocedure voor nieuwe peers. Je kunt de blockchain dan precies zo inrichten als voor de door jou beoogde toepassing ideaal is, sommigen mogen de blockchain alleen raadplegen, anderen mogen ook wijzigingen aanbrengen die door andere peers goedgekeurd moeten worden. Een poging om het beste van twee werelden te combineren: niet de totale chaos van anonimiteit die de bescherming van het recht moet ontberen, maar wel het voordeel van robuuste gedistribueerde gegevensopslag. Dat is een permissioned blockchain, het tegenovergestelde van een permissionless of openbare blockchain.

Er zijn ook alternatieven bedacht voor het energie-slurpende en daardoor niet meer ecologisch verantwoorde proof-of-work minen, zoals proof-of-stake. Niet de rekenkracht maar de hoeveelheid cryptocurrency die een peer al heeft is dan bepalend voor het kunnen toevoegen van een nieuw blok.

En via een blockchain kun je niet alleen betalingen in en saldi van cryptocurrency bijhouden, maar op het grootboek kunnen ook rechten op allerlei zaken geregistreerd, bijgehouden en eventueel overgedragen worden. En zo gaan we naadloos over naar wat 'smart contracting' genoemd wordt: het gebruik van blockchaintechnologie voor het bijhouden van rechten op waardevolle zaken en voor het afhandelen van transacties met betrekking tot die waardevolle zaken.

Smart contracts

De term 'smart contracts' is volgens mij misleidend en onjuist. Het gaat volgens mij niet over contracten, maar over de geautomatiseerde uitvoering van eerdere afspraken tussen partijen. Of het gaat over een soort openbaar aanbod, dat je kunt aanvaarden door een bepaalde actie te verrichten (normaal gesproken: betalen). Vergelijkbaar met een frisdrankautomaat.⁶ De overeenkomst ontstaat dan door de actie (acceptatie) van de wederpartij.

En in mijn optiek is er niets 'smarts' aan de ijzeren-heinige, rücksichtslose uitvoering van een computerprogramma – zeker niet in vergelijking mensen die met goedschiks of kwaadschiks gebruik van hun gezonde verstand al dan niet aan hun contractuele verplichtingen voldoen. Maar goed, het is een inmiddels ingeburgerde term en hij bekt lekker, dus daar houden we het maar bij.⁷

Een smart contract is een computerprogramma. Zo'n programma is opgebouwd uit een aantal regels in een 'als - dan' vorm: als aan bepaalde condities voldaan is volgt een bepaalde actie. Bijvoorbeeld: als een betaling ontvangen is, wordt een bepaalde zaak geleverd (of andersom). Dat programma 'is' dan een account op een blockchain. Het account heeft een bepaald bedrag in de valuta van de desbetreffende blockchain en handelt precies zoals het geprogrammeerd is. Voor gebeurtenissen die een bepaalde conditie moeten triggeren die niet door het programma zelf vastgesteld kunnen worden kunnen zogenaamde Oracles gebruikt worden: instanties of mensen die geautoriseerd zijn om bepaalde feitelijke vaststellingen te doen (daar zijn ze weer: deTTP's!).

Eenmaal losgelaten op de blockchain is de executie van zo'n programma niet te stoppen. Als de condities zich voordoen, dan zal de actie volgen, wat er ook verder aan de hand is. Voor foutjes en fouten, wilsgebreken, gewijzigde omstandigheden, voortschrijdend inzicht en al dat soort flauwekul is geen plaats. Tenuitvoerlegging is automatisch en dus gegarandeerd. Zo kun je met onbekende partijen over de hele wereld zaken doen, zonder bankgaranties of bemoeienis anderszins van TTP's.

3. Waarom zou je 't doen?

Dat zijn meteen de voordelen: ouderwetse, dure en inefficiënte tussenpersonen zoals banken, notarissen en andere juristen zijn overbodig. Nakoming is gegarandeerd, het is in zekere zin veilig en transparant. De nadelen zijn het spiegelbeeld hiervan: er is ook geen derde partij meer om op terug te vallen, nakoming kan niet worden tegengehouden.

Bij smart contracts wordt door de term alleen al in de eerste plaats gedacht aan privaatrechtelijke toepassingen, in de sfeer van de uitvoeringen van overeenkomsten. Maar als het gaat over het bijhouden van rechten op zaken, of het triggeren van verplichtingen door bepaalde gebeurtenissen, dan zijn er misschien ook nuttige publiekrechtelijke toepassingen. Ik denk aan het bijhouden van het kadaster, of het ontstaan van betalingsverplichtingen (bijvoorbeeld belasting of heffingen) die ontstaan bij bepaalde feitelijke handelingen (parkeren, afval genereren). Dat opent misschien de mogelijkheid voor bepaalde bestuursrechtelijke toepassingen?

We hebben deze discussie, zij het in iets andere termen, eerder gehad. In de jaren '90 van de vorige eeuw waren er bij sommigen hooggespannen verwachtingen van gebruik van zogenaamde juri-

6. Een vergelijking die ook Nick Szabo, die de term smart contract voor het eerst gebruikte, maakt. Zie Nick Szabo, The Idea of Smart Contracts, <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>.

7. Smart Contract Werkgroep, Smart contracts als specifieke toepassing van de blockchain-technologie, Dutch Blockchain Coalition, (<https://www.dutchdigitaldelta.nl/uploads/pdf/Smart-contract-rapport-DBC.pdf>). Can smart contracts be legally binding con-

tracts? An R3 and Norton Rose Fulbright White paper, <http://www.nortonrosefulbright.com/files/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf>. Whitepaper Juridische aspecten van Blockchain, Pels Rijcken, aan te vragen via <https://www.pelsrijcken.nl/actueel/publicaties/whitepaper-juridische-aspecten-van-blockchain/>. E. Tjong Tjin Tai, 'Smart contracts en het recht', *NJB* 2017, 92(3), 176-183. [146].

dische kennissystemen of expertsystemen.⁸ Juridisch redeneren zou gereduceerd kunnen worden tot toepassing van vergelijkbare als .. dan regels. Rechtsregels zouden geformaliseerd kunnen worden in deze zogenaamde productieregels, en de jurisprudentie waarin deze regels uitgelegd en toegepast worden zou als grondstof voor zelflerende systemen op basis van deze regels gebruikt kunnen worden zodat ze mee kunnen evolueren met de rechtsontwikkeling.⁹ Ook toen werd door sommigen betoogd dat het recht zich niet laat vangen in productieregels, dat er zogenaamde hard cases zijn die een menselijke beoordeling vergen, en dat het onderscheid tussen clear en hard cases niet door een geautomatiseerd systeem zelf gemaakt kan worden.¹⁰ Met verwijzing naar de discussie tussen Hart en Dworkin over de bepaaldheid van het recht en de rol van morele argumenten (die wel of niet tot het rechtssysteem zelf behoren) bij de toepassing van rechtsregels.¹¹

Hoewel de overspannen verwachtingen over juridische expertsystemen niet helemaal waargemaakt werden, hebben computerprogramma's natuurlijk toch hun intrede gedaan in de rechtstoepassing.¹² Niet alleen ter ondersteuning van administratieve processen, maar ook om beslissingen te nemen met rechtsgevolgen. Tegenwoordig wordt daar ook weer voorzichtig de term AI bij gebruikt, en de fancy newspeak term is dan 'legal tech'.

Maar dan hebben we het nog steeds 'gewoon' over het inzetten van een computerprogramma bij het

uitvoeren of toepassen van regels – hetzij publiekrechtelijke regels hetzij regels zoals die voortkomen uit een privaatrechtelijke overeenkomst. Waarom zou je het computerprogramma dat die regels uitvoert dan wel toepast in hemelsnaam als smart contract op een blockchain implementeren? Omdat de voordelen die implementatie als smart contract met zich meebrengt voor sommige toepassingen belangrijk zijn. De voordelen kwamen hierboven al even aan de orde: geen afhankelijkheid van een TTP, transparantie, nakoming is gegarandeerd. Je kunt dan denken aan toepassingen als verzekeringen,¹³ peer-to-peer lending,¹⁴ crowdfunding,¹⁵ vastgoedbeleggingen,¹⁶ IE-licenties,¹⁷ en bijhouden van zorg-administratie.¹⁸ Misschien zijn er voor dat soort toepassingen inderdaad goede redenen om smart contracts te gebruiken – al vraag ik me soms wel af of het niet beter en gemakkelijker zonder blockchain zou kunnen. Maar goed, dat is aan de vrije markt om uit te proberen – wellicht een uitgelezen kans voor slimmeriken met een briljant idee om snel rijk te worden?

Een moeilijk punt bij smart contracts is de verbinding met de fysieke wereld. Als er Oracles nodig zijn om een bepaalde actie te triggeren, ben je in zekere zin toch weer overgeleverd aan TTP's met risico's van fraude en hacking. Maar als de verbinding met de fysieke wereld nou met behulp van apparaten gelegd kan worden die tegenwoordig met de term 'Internet of Things' (IoT) aangeduid worden, dan opent zich wellicht wel een scala aan mogelijkheden. We pakken onze glazen bol erbij.

Het standaardvoorbeeld van IoT dat meteen bij mij opkomt is de smart koelkast die op het moment dat de voorraad van een of ander artikel (bier of cherytomaatjes) onder een bepaald minimum komt (en dat weet de koelkast omdat alle verpakking zijn uitgerust met een RFID-chip) automatisch een bestelling doorgeeft zodat later die dag de bezorgdienst van de supermarkt (jongeman op een vrachtwagen of wellicht een automatisch bezorgkarretje of drone) zorgt dat alles weer goed komt. Prima, leuk – maar waarom zou je zoiets op een blockchain doen? Spreek dat gewoon lekker af met je plaatselijke supermarkt.¹⁹

De blockchain komt van pas als je ook met onbekenden zaken wilt kunnen doen, via zo'n openbaar-aanbod-smart contract. In plaats van een schaarse parkeerplaats bezet te houden kan de

8. A.W. Koers, *Juridische Informatica, Spelen met de computer, of spelen met het recht, Inaugurale Rede*, Alphen aan den Rijn: Samsom H.D. Tjeenk Willink 1987; H.J. van den Herik, *Kunnen computers rechtspreken? Inaugurale Rede*, Arnhem: Gouda Quint 1991.
9. Zie onder andere A. van der Lieth Gardner, *An Artificial Intelligence Approach to Legal Reasoning*, Cambridge, Massachusetts: The MIT Press 1987; J.C. Hage, 'Themis als robot, Juridische expertsystemen tussen trivialiteit en onbetrouwbaarheid', *RM Themis* 1987, pp. 238-248; H. Prakken, *Logical tools for modelling legal arguments*, proefschrift VU Amsterdam, 1993; Arno R. Lodder, *DiaLaw, On legal justification and dialog games*, proefschrift Universiteit Maastricht, 1998; M.C.M. Weusten, *De bouw van juridische kennissystemen: Building legal knowledge based systems: KRT: methodology and tools: KRT: methodologie en gereedschap*, proefschrift Universiteit Utrecht 1999.
10. Tina Smith, *Legal Expert Systems: Discussion of Theoretical Assumptions*, proefschrift Universiteit Utrecht, 1994.
11. H.L.A. Hart, *The Concept of Law*, Oxford: Clarendon Press 1961, R. Dworkin, *Law's Empire*, Cambridge, Massachusetts: Belknap Press 1986.
12. C.N.J. de Vey Mestdag, *Juridische kennissystemen, rekentuig of rekenmeester? Het Onderbrengen van Juridische Kennis in een Expertsystem voor het Milieuvergunningenrecht*, Deventer: Kluwer Academic Publishers 1997; T. van der Linden-Smith, *Een duidelijk geval: Geautomatiseerde afhandeling*. Vol. 41, Iter-reeks 2001; Marlies van Eck, *Geautomatiseerde ketenbesluiten & rechtsbescherming. Een onderzoek naar de praktijk van geautomatiseerde ketenbesluiten over een financieel belang in relatie tot rechtsbescherming*, proefschrift Tilburg 2018.

13. <https://blog.jincor.com/smart-contract-examples-can-it-really-improve-your-business-4a5821575fe9>.
14. <https://lendoit.com/>.
15. <https://www.uitlegblockchain.nl/category/crowdfunding/>.
16. <https://www.blandlord.com/>.
17. <http://www.ie-forum.nl/artikelen/binde-de-knock-auteursrechtdebat-blockchain-voor-bij-de-hype-hardwells-blockchain-release>.
18. <https://www.istandaarden.nl/izo/innovaties/blockchain-mijn-zorg-log>.
19. En ook zoiets hebben we (veel) eerder gezien, in de vorm van de aan Electronic Data Interchange ten grondslag liggende interchange agreements.

zelfrijdende auto die jou op je werk afgezet heeft, zichzelf anderszins nuttig maken. Andermans kinderen naar de opvang brengen, bestellingen afleveren, verzin maar iets.²⁰ Een smart contract maakt de organisatie en de afhandeling van dit soort transacties mogelijk. Een sharing economy zonder tussenpersonen als AirBNB en Uber, maar ècht peer-to-peer. Sharing economy tussenpersonen zijn tenslotte ook TTP's, die zich bemoeien met de inhoud van de overeenkomst, die gelden doorsluisen (en een deel zelf inpikken), die fraude kunnen plegen, failliet kunnen gaan en gehackt kunnen worden.

Dàn ziet de wereld er anders uit. Fysiek, en ook juridisch. De mogelijkheden om wanprestatie te plegen zijn (veel) beperkter en dus zijn de risico's (veel) lager. Door het wegvallen van de tussenpersonen zijn de transactiekosten ook (veel) lager.

We maken gauw een screenshot van het beeld uit de glazen bol voordat het vervaagt. En we blijven in verwarring achter.

4. Uitdagingen voor het recht

Is er bij gebruik van smart contracts nog wel plaats voor ons goede oude verbintenissenrecht, met z'n verworven subtiele correctiemechanismen als goede trouw, redelijkheid en billijkheid, opgewekte verwachtingen en schijn, gegaste uien,²¹ Haviltex?²² Of is dat overrated folklore?

Zoals altijd: dat hangt ervan af. Bijvoorbeeld van wie je contractspartijen zijn en of zij goed geïnformeerd hebben gekozen voor een smart contract. Gaat het om grote internationale business-contracten? Dan niet piepen: Mark = Mark.²³ Maar anonimiteit maakt dat je niet weet met wie je te maken hebt. Moeten we zwakke partijen zoals consumenten beschermen? Moeten we mensen tegen hun eigen hebzucht en/of dommigheid beschermen?

Wat zijn bestuursrechtelijke haken en ogen van gebruik van smart contracts door overheden? Wie zijn de peers van de betreffende blockchains? Kan de burger nog wel tegenbewijs leveren als de 'blockchain says no'? Is dat wel behoorlijk besturen?

Hoe gaan we ooit compliant zijn met de AVG als 'op' de blockchain persoonsgegevens verwerkt worden?²⁴ Of staan er op de blockchain alleen links naar persoonsgegevens die elders in de cloud ver-

sleuteld opgeslagen zijn? En is dat dan wel AVG-proof?

Tja, het recht. Waarom hebben we dat ook al weer? Het recht moet zorgen voor rechtvaardigheid (maar wat dat inhoudt is onderwerp van voortdurende discussie), misdaad bestrijden (op straffe van verlies van legitimiteit), de democratische rechtsstaat beschermen (of sowieso de staat – hoe gaan we nog belasting heffen?), en natuurlijk mensenrechten zoveel mogelijk verwezenlijken: non-discriminatie, privacy om maar 's wat te noemen. Hoe gaan we dat doen op de Blockchain?

Ik weet het niet. Is dit nu echt iets nieuws onder de zon dat noopt tot heroverweging of misschien zelfs tot aanpassing van het bestaande juridisch instrumentarium? Of gaat het slechts om schaalvergroting van issues zoals anonimiteit, grensoverschrijdendheid, consumentenbescherming, waar we op ons goeie ouwe Internet ook al zo goed en zo kwaad als het gaat mee dealen? Dan is er nog het fenomeen dat 'scale matters',²⁵ een kwantitatief verschil kan zo groot worden dat het een kwalitatief verschil wordt.

In een voorgenomen vervolgartikel wil ik proberen om deze uitdagingen voor het recht in kaart te brengen. Volgens mij zijn er voorlopig geen zorgen over werkgelegenheid voor juristen. We moeten hiermee aan de gang, en ik vermoed dat we juristen nodig hebben die de code van een smart contract kunnen lezen en schrijven. Conclusie: dit is volgens mij ècht een technologische ontwikkeling die nu nog onvermoede mogelijkheden biedt – en waar juristen zich hoognodig mee moeten bemoeien. Misschien om vast te stellen dat het allemaal wel meevalt. Maar ook om die conclusie te kunnen trekken is het nodig om je er goed in te verdiepen. Wordt vervolgd!

20. Voorbeeld ontleend aan de reactie van Oelfier op 16 januari 2018 op het blog van Arnoud Engelfriet: Welke rol gaan smart contracts spelen in het recht?, <https://blog.iusmentis.com/2018/01/12/welke-rol-gaan-smart-contracts-spelen-recht/#comments>.

21. HR 7 maart 1969, NJ 1969, 249 (Gegaste uien)

22. HR 13 maart 1981, NJ 1981/635 (Haviltex). Zie ook: J.B. Schmaal & E.M. van Genugten, 'Smart contracts en de Haviltex-norm', *Tijdschrift voor Internetrecht* 2017-1, pp. 12-17.

23. HR 2 januari 1931, NJ 1931, 274 (Mark = Mark)

24. V.I. Laan, 'Privacy en blockchain: wanneer is er voor wie privacywerk aan de winkel?' *IR* 2017, nr. 1, pp. 4-11.

25. D. Post, 'Against "Against Cyberanarchy"' (2002) 17 *Berkeley Technology Law Journal* 1-23.